Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A system for providing quarantine on a network comprising:

a client device seeking access to a network resource, the client device configured to:

perform a first plurality of checks specified by a first manifest,

store a first status report at the client device, the first status report specifying results of the first plurality of checks, and

send a Bill of Health (BoH) request that contains the first status report;

a first server device that:

receives the BoH request sent by the client device,

determines whether the first status report indicates that the client device passed all of the checks specified by a second manifest that specifies a second plurality of checks that the client device must perform,

sends to the client device ~~for providing the client with a~~ the second manifest ~~of checks~~ when the first status report indicates that the client device did not pass all of the checks specified by the second manifest, [[and]]

receives, from the client device, a second status report that indicates results of the client device performing the second plurality of checks,

stores a Bill of Health (BoH) for the client device when the second status report indicates that the client device passed all of the checks in the second plurality of checks, the BoH comprising a creation time of the BoH, an expiration date of the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

if the results of the second plurality of checks show that the client device passed all of the checks in the second plurality of checks, ~~manifest of checks is passed by the client, for providing~~ sends, to the client device, a certificate that provides proof that the client device possesses a required configuration, the certificate comprising a serial

number of the BoH, an address of the first server device, and a digital signature; and

a second server device that:

receives a request for access to the network resource from the client device, the request including the certificate,

uses the serial number in the certificate and the address of the first server device to retrieve the BoH from the first server device,

uses the digital signature of the certificate to determine whether any part of the certificate has been modified after the certificate was issued by the first server device,

after retrieving the BoH, uses the integrity check to determine whether the BoH has been tampered,

determines whether the expiration date of the BoH has passed,

determines whether the manifest version identifier identifies a most recent manifest version number,

provides ~~for providing~~ access to the network resource when the second server device determines that the certificate has not been modified after the certificate was issued by the first server device, that the BoH has not been tampered, that the expiration date for the BoH has not passed, and that the manifest version identifier specifies the most recent manifest version number,

wherein the second server device denies the client device access to the network resource when the second network server device determines that the certificate has been modified after the certificate was issued by the first quarantine server device, that the BoH has been tampered, that the expiration date for the BoH has passed, or that the manifest version identifier does not identify the most recent manifest version number; ~~until the client presents the proof that the client possesses the required configuration;~~

wherein the client device periodically requests that the certificate ~~proof~~ be updated by the first server device, regardless of whether the client device sends further requests for access to the network resource to the second server device.

2. (Currently Amended) The system of claim 1, wherein the second plurality of checks includes at least one of checks for: installed software, a software version, an installed patch, an

installed anti-virus system, an anti-virus state, a firewall state, an installed service, file sharing, a registry value, a registry key, and a file system state.

3. (Currently Amended) The system of claim 1, wherein the client device comprises delegates that perform the checks in the first plurality of checks and the second plurality of checks. ~~manifest of checks.~~

4. (Currently Amended) The system of claim 1, wherein ~~the client sends the first server the result the checks, and the first server provides the client with a certificate certifying that the client possesses the required configuration if the client passes the checks, and~~ the client device stores a copy of the certificate in a database.

5. (Canceled)

6. (Canceled)

7. (Currently Amended) The system of claim 1, wherein if the client device cannot provide proof that the client device possesses the required configuration, the second server device directs the client device to the first server device.

8. (Canceled)

9. (Currently Amended) The system of claim [[8]] 1, wherein the second server device includes a second database that is a replica of the first database, wherein the client device proves possession of the required configuration by sending the second server device the serial number of the BoH, ~~unique identifier,~~ wherein the second server device compares the ~~unique identifier~~ serial number of the BoH to [[the]] a unique identifier stored with the certificate in the second database.

10. (Currently Amended) The system of claim 1, wherein the first server device requests

a software inventory from the client device and ~~provides~~ sends, to the client device, software necessary for the required configuration.

11. (Currently Amended) The system of claim 1, further comprising an access point for mediating communication between the client device and the second server device, wherein the second server device is protected by a firewall.

12. (Currently Amended) The system of claim 1, wherein the first server device and ~~is a service executing on a computing device and~~ the second server device are ~~is a service also executing on the~~ one computing device.

13. (Currently Amended) A method for a client device to acquire access to a network resource, comprising:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from the [[a]] first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration;

performing, at the client device, the checks in the second manifest of checks; [[and]]

sending, from the client device to the first server device, a second status report that indicates [[the]] results of the checks of the second manifest ~~to the first server~~;

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses [[of]] the required configuration, ~~from the first server;~~

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

~~requesting~~ sending, from the client device to a second server device that controls access to the network resource, a request for access to the network resource; ~~from a second server controlling access to the network resource;~~

sending, from the client device to the second server device, the certificate; ~~proof of the required configuration to the second server; and~~

receiving, at the client device, access to the network resource when the certificate has not been modified after the certificate was issued by the first server device, the BoH has not been tampered, the expiration date for the BoH has not passed, and the manifest version identifier of the BoH identifies a most recent manifest version number;

periodically requesting, from the client device, that the ~~proof~~ certificate be updated by the first server device, regardless of whether the client device sends further requests for access to the network resource to the network server device.

14. (Currently Amended) The method of claim 13, further comprising:

receiving, at the client device, a request for a software inventory from the first server device;

receiving, at the client device, software necessary for the required configuration; and

installing the software at the client device.

15.-17. (Canceled)

18. (Currently Amended) The method of claim 13, wherein the first server device ~~is a service executing on a computing device and~~ the second server device are ~~is a service also executing on the~~ one computing device.

19.-22. (Canceled)

23. (Currently Amended) A method for quarantining a client device from access to a network resource, comprising:

receiving, at a first server device, a request for access to the network resource from the client device;

receiving, at the first server device from the client device, a certificate that provides proof ~~from the client~~ that the client device has [[of]] a required configuration, wherein the certificate specifies a serial number of a Bill of Health (BoH) generated by a trusted server device that only generates the BoH when the trusted server device receives, from the client device, a status report that indicates results of checks specified in a manifest sent to the client device by the trusted server device and the results of the checks show that the client device passed all the checks;

sending, from the first server device to the trusted server device, a request for the BoH, the request specifying the serial number of the BoH;

receiving, at the first server device, the BoH, the BoH specifying a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that specifies a version number of the manifest, and an integrity check;

validating, at the first server device, the ~~proof by comparing the proof to information obtained from a trusted server~~ certificate when the certificate has not been modified after the certificate was issued by the trusted server device, the BoH has not been tampered, the expiration date of the BoH has not passed, and the manifest version identifier specifies a most recent manifest version number;

if the ~~proof~~ certificate is valid, allowing the client device access to the network resource;

if the ~~proof~~ certificate is invalid, denying the client device access to the network resource; and

wherein the trusted server device periodically receives from the client device ~~receiving~~ a request that the proof be updated ~~by the first server~~, regardless of further requests for access to the network resource.

24. (Currently Amended) The method of claim 23, further comprising, if the ~~proof~~ certificate is invalid, directing, at the first server device, the client device to the trusted server device so that the required configuration is obtained.

25.-27. (Canceled)

28. (Currently Amended) ~~A computer program product for use in a computer system, the computer program product comprising one~~ One or more computer readable storage media having computer-executable instructions ~~for implementing~~ that, when executed by a processing unit in the client device, cause the client device to perform a method for a client device to acquire access to a network resource, the method comprising the steps of:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from a first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration of installed software;

performing, at the client device, the checks in the second manifest of checks; [[and]]

sending a second status report that indicates [[the]] results of the checks of the second manifest from the client device to the first server device;

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses [[of]] the required configuration,

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check; ~~from the first server;~~

sending, from the client device to a second server device that controls access to the

network resource, a request to ~~requesting~~ access to the network resource; ~~from a second server controlling access to the network resource;~~

sending, from the client device to the second server device, the certificate ~~proof of the required configuration to the second server~~;

receiving, at the client device, access to the network resource when the certificate has not been modified after the certificate was issued by the first server device, the BoH has not been tampered, the expiration date for the BoH has not passed, and the manifest version identifier of the BoH identifies a most recent manifest version number; and

periodically sending, from the client device to the first server device, a request to update ~~requesting that~~ the proof ~~be updated by the first server~~, regardless of further requests for access to the network resource.

29. (Currently Amended) A system for a client device to acquire access to a network resource, comprising:

a processing unit; and

a memory coupled with and readable by the processing unit and having stored therein instructions which, when executed by the processing unit, cause a module to perform the following acts:

performing, at the client device, a first plurality of checks specified by a first manifest;

storing a first status report at the client device, the first status report specifying results of the first plurality of checks;

sending a Bill of Health (BoH) request that contains the first status report from the client device to a first server device;

receiving, at the client device, a second manifest of checks from a first server device when the first server device determines that the first status report indicates that the client device did not pass all of the checks specified by the second manifest, wherein the checks of the second manifest determine whether the client device possesses a required configuration;

performing, at the client device, the checks in the second manifest of checks;

[[and]]

sending, from the client device to the first server device, a second status report that indicates [[the]] results of the checks of the second manifest; ~~to the first server;~~

receiving, at the client device from the first server device, a certificate that provides proof that the client device possesses [[of]] the required configuration, ~~from the first server;~~

wherein the certificate comprises a serial number of a BoH for the client device stored at the first server device, an address of the first server device, and a digital signature, and

wherein the BoH comprises a creation time of the BoH, an expiration date for the BoH, a manifest version identifier that identifies a version number of the second manifest, and an integrity check;

storing the ~~proof~~ certificate at the client device;

sending, from the client device to a second server device that controls access to the network resource, a request to ~~requesting~~ access [[to]] the network resource ~~from a second server controlling access to the network resource~~;

determining, at the client device, whether the ~~proof~~ certificate stored at the client device is valid;

sending, from the client device to the first server device, a request to update the proof ~~requesting,~~ if the ~~proof~~ certificate is no longer valid~~, the first server to update the proof~~;

sending, from the client device to the second server device, the ~~proof~~ certificate of the required configuration ~~to the second server~~; and

periodically sending, from the client device to the first server device, requests to update ~~requesting that~~ the certificate, ~~proof be updated by the first server,~~ regardless of further requests for access to the network resource.